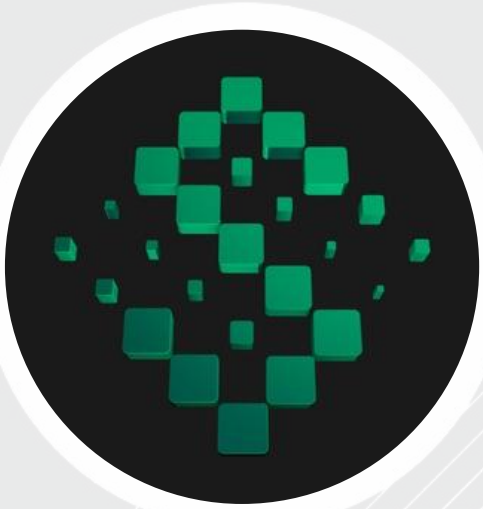
SPYWOLF

Security Audit Report



Completed on

June 11, 2022

MADE IN USA 🇺🇸

OVERVIEW

This audit has been prepared for **SAFUFIDE** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

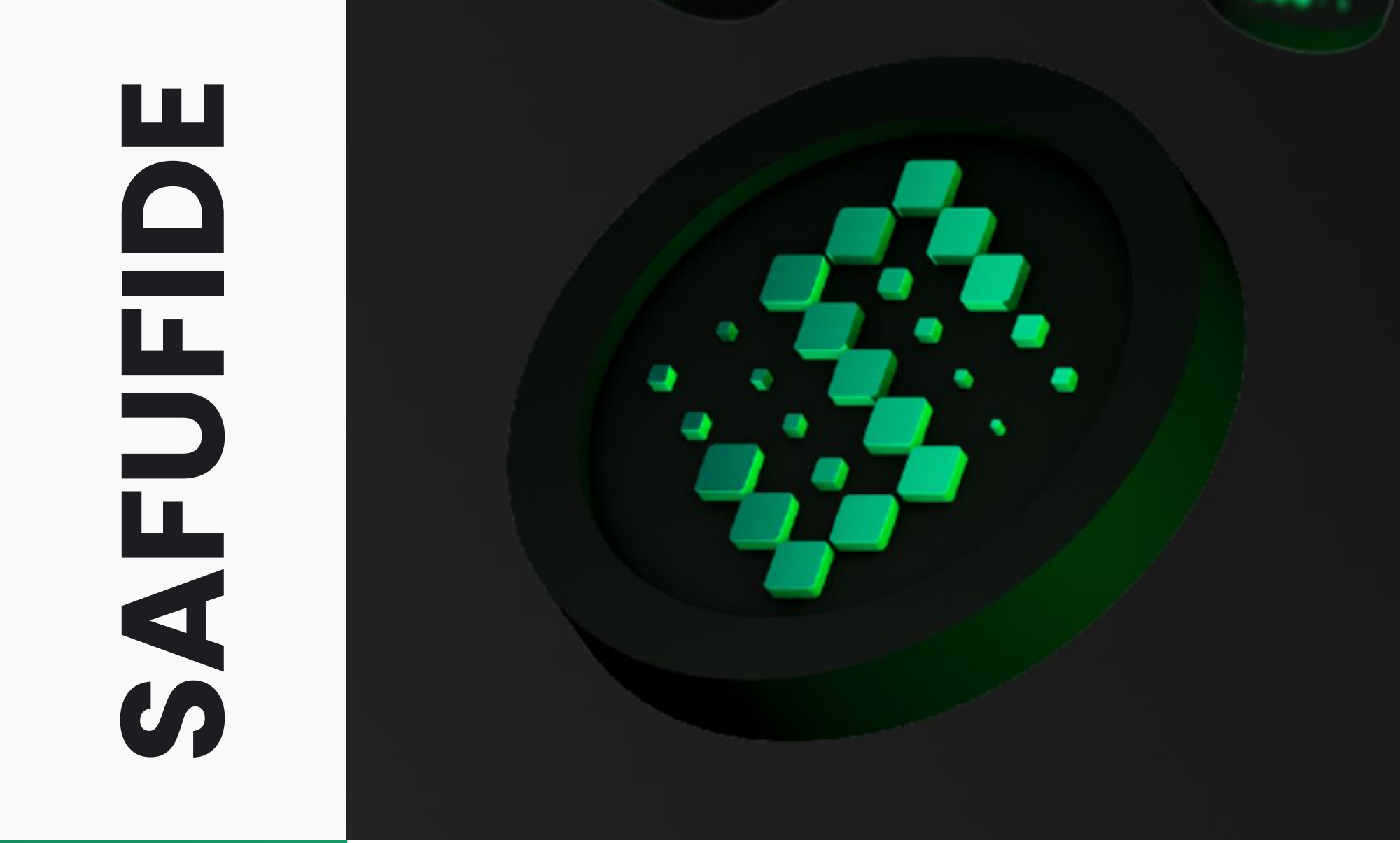
The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03-04
Featured Wallets	05
Vulnerability Check	06
Threat Levels	07
Found Threat	08-09
Good Practices	10
Tokenomics	N/A
Team Information	11
Website Analysis	12
Social Media & Online Presence	13
About SPYWOLF	14
Disclaimer	15

SAFUFIDE



PROJECT DESCRIPTION

SafuFide Safe-Sig is a trusted platform to protect and manage digital assets on Binance Smart Chain, that will include multi-chain in the near future. Built on the Gnosis open source protocol, they are focusing on individuals and their long term plans is to focus on projects (apps, DAOs, auditing contracts, launchpad, etc). Multisig wallets (SafuFide) will be able to be used to protect not just the assets in wallets but also used to protect the smart contracts by ensuring that it would take multiple signatures to change the contract.

Release Date: Sep 1, 2021

Category: Wallet

CONTRACT INFO

Contract Name
CataBoltStaking

Symbol
N/A

Contract Address
0xd9cEE5d24B06B3f63B3a8d8e8C081C78319665e8

Network
Binance Smart Chain
TESTNET

Language
Solidity

Deployment Date
June 09, 2022

Verified?
Yes

Total Supply
n/a

Status
Deployed

TAXES

Buy Tax
n/a

Sell Tax
n/a

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(AS OF June 11, 2022)

Liquidity

n/a

Burn

n/a

Status:

Deployed on TESTNET!

MaxTxAmount
n/a

Additional info

MinLockTime
604800

MinStakingAmount
1,000,000

TokenAddress
0x00c809f449c240b6e1ff6cd070c88f77ddb61f08

LP Address(es)

n/a (Staking contract)

TOKEN TRANSFERS STATS

Transfer Count	TESTNET
Uniq Senders	TESTNET
Uniq Receivers	TESTNET
Total Amount	TESTNET
Median Transfer Amount	TESTNET
Average Transfer Amount	TESTNET
First transfer date	TESTNET
Last transfer date	TESTNET
Days token transferred	TESTNET

SMART CONTRACT STATS

Calls Count	TESTNET
External calls	TESTNET
Internal calls	TESTNET
Transactions count	TESTNET
Uniq Callers	TESTNET
Days contract called	TESTNET
Last transaction time	TESTNET
Created	TESTNET
Create TX	TESTNET
Creator	TESTNET

FEATURED WALLETS

Owner address	0x06c0313ea7e4f02d5a3077b292f104aecfbd5404
LP address	**Staking contract**

TOP 3 UNLOCKED WALLETS

1

n/a

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Medium risk

Owner can set withdrawal lock time period without limitation.

```
function setMinLockTime(uint256 duration) public onlyAdmin {
    minLockTime = duration;
}
function withdraw(uint256 amount) public updateReward(msg.sender) {
    require(block.timestamp - depositDates[msg.sender] > minLockTime, "<lockTime");
    IERC20(tokenAddress).transfer(msg.sender, amount);
    super.withdraw(amount, msg.sender);
    emit Withdraw(msg.sender, amount);
}
function exit() public updateReward(msg.sender) {
    require(block.timestamp - depositDates[msg.sender] > minLockTime, "<lockTime");
    uint256 reward = earned(msg.sender);
    uint256 balance = balanceOf(msg.sender);
    uint256 amount = reward + balance;
    require(amount > 0, 'amount=0');
    IERC20(tokenAddress).transfer(msg.sender, amount);
    rewards[msg.sender] = 0;
    super.withdraw(balance, msg.sender);
    emit Exit(msg.sender, amount);
}
```

- Recommendation:
  - Good practice is to set limitations on user restrictions like withdraw time from staking contracts.

FOUND THREATS

⚠ Low Risk

Owner can change rewards rate.

```
function setDuration(uint256 duration) public onlyAdmin {
    DURATION = duration;
}
function setMinStakingTransfer(uint256 _minStakingTransfer) public onlyAdmin {
    minStakingTransfer = _minStakingTransfer;
}
function notifyRewardAmount(uint256 reward) public updateReward(address(0)) onlyReward{
    if (reward == 0) {
        reward = minStakingTransfer;
    }
    if (block.timestamp >= periodFinish) {
        rewardRate = reward.div(DURATION);
    } else {
        uint256 remaining = periodFinish.sub(block.timestamp);
        uint256 leftover = remaining.mul(rewardRate);
        rewardRate = reward.add(leftover).div(DURATION);
    }
    lastUpdateTime = block.timestamp;
    periodFinish = block.timestamp.add(DURATION);
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

SAFUFIDE

GOOD PRACTICES FOUND

- ✔ The owner cannot stop or pause the contract
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

THE TEAM

✅ The team at SAFUFIDE is publicly doxxed.

They are part of the NEXUS ECOSYSTEM, a chain of DeFi utilities and cryptocurrency solutions that is defined by its passion for solving problems, creating opportunity and helping build wealth within the cryptocurrency realm.

PETER GANTNER
Founder / CEO

DOUG KYLE
Founder / CTO

CORY MORAN
Founder / Graphic designer/ Social media

DAWN CLIFTON
Founder / Lead Software Development

RHONDA BENBO
Founder / Marketing

DEBORAH CASWELL
Tour Guide/Video Production

CANDIS LUTHER
Onboarding Support Team

STEVE KANELOS
Onboarding Support Team

SHARONA LABROSSE
Customer Service

BRENDAN DUFF
Business Operations/Algorithms Development

WEBSITE

Website URL
https://safufide.io

Domain Registry
https://www.godaddy.com

Domain Expiration
May 3, 2025

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

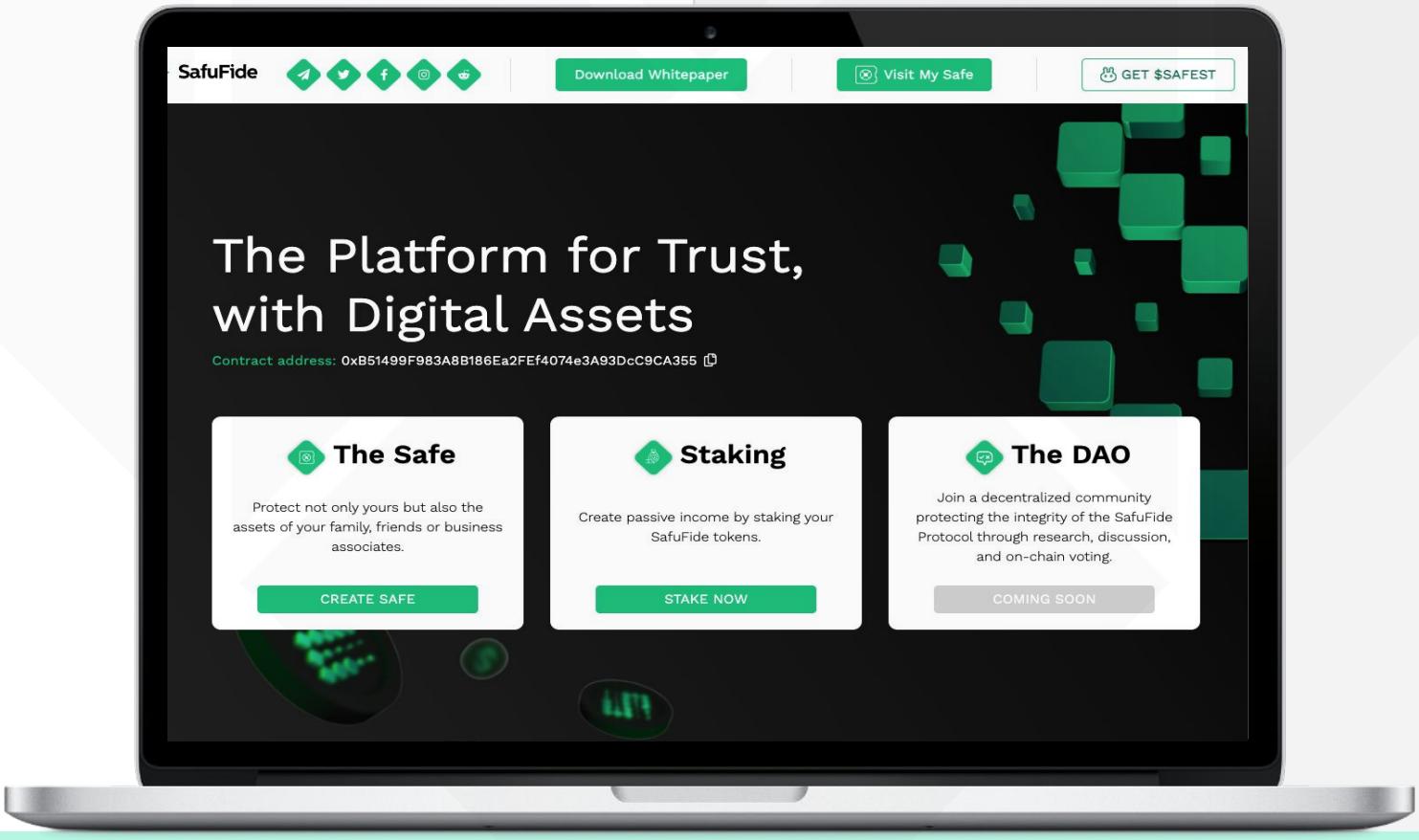
Design
Very nice color scheme and overall layout.

Content
The information helps new investors understand what the product does right away. No grammar errors found. .

Whitepaper
Well written but a bit short

Roadmap
Yes

Mobile-friendly?
Yes

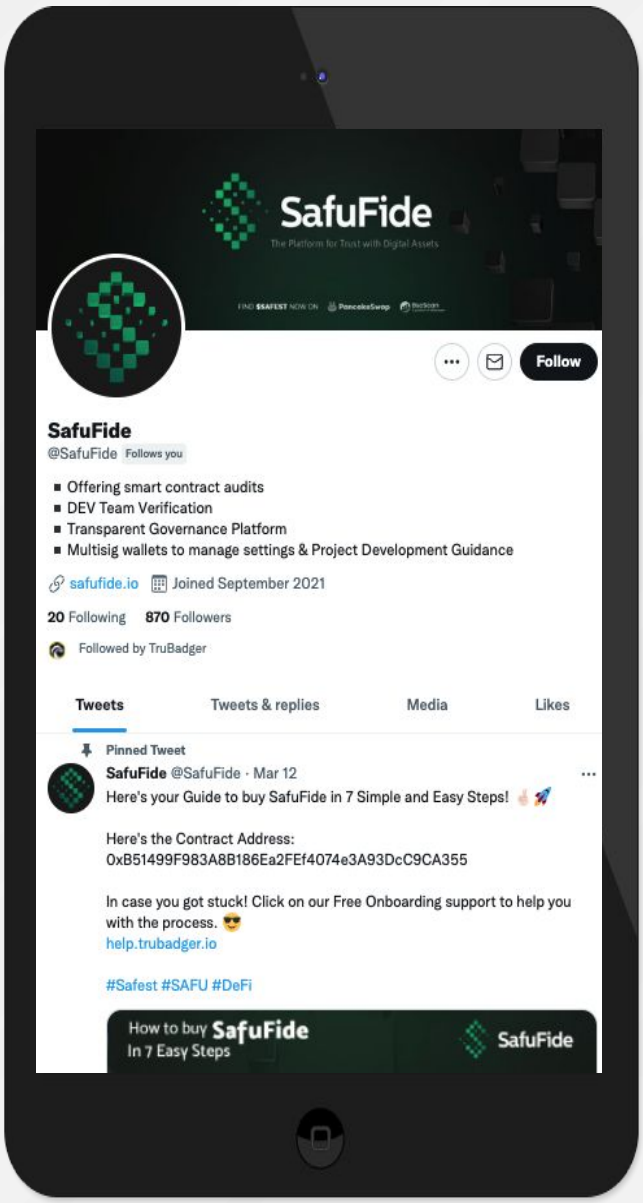


safufide.io

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS



Twitter

https://twitter.com/SafuFide

- 1 078 followers
- Active
- Posts every few days

Discord

- Not available

Telegram

https://t.me/SafuFideOfficial

- 742 members
- Announcement channel, no chat

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.